

ПОЛИС ОМС КАК ПРИМАНКА: как защититься от самых опасных схем телефонных аферистов

Мошенники всё активнее используют тему обязательного медицинского страхования, чтобы получить доступ к банковским картам граждан или лично к кабинету на «Госуслугах», – звонят, присылают фишинговые сообщения и под разными предлогами выпытывают коды и персональные данные.

Начальник отдела информационной безопасности ТФОМС Кемеровской области – Кузбасса **Михаил МАРКОВИЦЕВ** рассказал не только о наиболее типичных сценариях мошенничества, но и поделился проверенными практическими инструкциями: что делать, если вы уже ответили на звонок злоумышленников, какие шаги предпринимать, чтобы минимизировать потери, и как защитить своих технически менее подкованных родственников.

– Насколько серьёзна сейчас проблема мошенничества, связанного с системой ОМС?

– Преступники целенаправленно используют для обмана сферу здравоохранения и ОМС, потому что она касается практически каждого человека. Финансовые потери россиян исчисляются баснословными суммами. По данным Центробанка, в 2025 году только через банковские операции злоумышленники похитили у россиян более 29 млрд рублей, общие же потери, по разным источникам, составляют не менее 295 млрд рублей.

Эта статистика лишь верхушка айсберга: многие граждане предпочитают не обращаться в правоохранительные органы, если сумма утраты небольшая, а значит, реальное число пострадавших и объём ущерба выше. Помимо прямых финансовых потерь, остаётся невидимый ущерб – утечка персональных данных и их дальнейшее использование для целевых атак.

– Какие сценарии чаще всего используют злоумышленники, когда «работают» через тему ОМС?

– Одна из самых распространённых схем – это «замена полиса ОМС». Мошенники звонят якобы из страховой компании, территориального фонда ОМС или с пор-

тала «Госуслуги» и сообщают, что нужно «продлить» или «заменить» полис ОМС на новый цифровой с QR-кодом. Предлагают скачать документ или говорят, что курьер может привезти полис к вам домой или на работу – достаточно назвать код из СМС-сообщения. Люди, боясь лишиться права на бесплатное медицинское обслуживание, верят аферистам и следуют их инструкциям. Между тем полис ОМС для россиян выдаётся бессрочно, бесплатно и не требует продления. Поэтому, как только услышали слова: «Заменить или продлить полис ОМС», сразу же кладите трубку.

Другой популярный прием – «запись на обследование без очереди». Аферисты звонят якобы из вашей поликлиники, предлагают пройти диспансеризацию, флюорографию или другое исследование без очереди и бесплатно за счет средств ОМС. Просят выбрать удобные дату и время, а для подтверждения записи назвать «номер талона» из СМС или перейти по ссылке. Делать этого ни в коем случае нельзя! Записываться на прием к врачу, диспансеризацию или обследование нужно только через официальные каналы: регистратуру поликлиники, единый телефонный номер 122, портал «Госуслуги», Медицинский портал Кузбасса (vrach42.ru) или чат-бот «Запись к врачу» в мессенджере МАХ.

В арсенале преступников есть и другие варианты обмана. Например, они просят назвать СНИЛС и код из СМС-сообщения, чтобы подтвердить согласие на «замену бумажной медицинской карты на электронную»; присылают сообщения о «плохих анализах» с требованием срочно оплатить лечение по реквизитам или QR-коду; отправляют фишинговые СМС-сообщения вроде «Ваш полис недействителен» или «Ваши анализы



Фото: magnific.com

готовы», в которых указан подставной номер для «консультаций».

Если вам на телефон поступило подобное сообщение, рекомендую проигнорировать его или самостоятельно позвонить в поликлинику или страховую медицинскую организацию, но не по указанному в сообщении телефону, а по телефону из официальных источников, например, с сайта организации.

Кроме телефонных звонков и СМС-сообщений, мошенники активно используют мессенджеры и соцсети: они создают фальшивые группы «для пациентов» и рассылают в них ссылки на «электронные полисы» или «срочные оповещения». Поэтому обязательно проверяйте, есть ли у такой группы отметка официального сообщества, и не вводите личные данные через незнакомые боты.

– Но ведь специалисты страховых компаний действительно могут позвонить своим застрахованным и пригласить на диспансеризацию. Как же отличить реальный звонок от мошеннического?

– Насторожить должны конкретные просьбы и действия звонящего. Если вам предлагают:

- назвать код, номер очереди или талона из СМС-сообщения;
- установить на телефон «приложение Минздрава»;
- перейти по присланной ссылке;
- перевести деньги на карту или по номеру телефона,

● предоставить удалённый доступ к экрану телефона.

Сразу же кладите трубку. Все эти фразы должны служить для вас стоп-сигналами.

Кроме того, телефонные мошенники мастерски оказывают психологическое давление, играя на базовых человеческих эмоциях:

● пугают граждан потерей всех сбережений, оформлением кредита на их имя, уголовным преследованием от имени полиции или ФСБ;

● требуют принять решение немедленно, не давая времени подумать, перепроверить информацию или посоветоваться с близкими;

● обращаются от имени «официальных» структур, представляются сотрудниками банков, Центробанка, правоохранительных органов или «Госуслуг», используют в разговоре строгий, официальный и уверенный тон, ссылаются на различные законы и приказы;

● убеждают, что вы сами «виноваты» в совершении подозрительной операции или утечке данных, и только срочное выполнение их инструкций спасет ситуацию;

● ошеломляют внезапной, тревожной новостью, чтобы отключить критическое мышление жертвы.

Хотелось бы отметить, что жертвами подобных манипуляций чаще всего становятся дети и пожилые люди. Поэтому необходимо заранее обсудить со своими близкими простые правила: никогда не передавать коды посторонним людям, не

устанавливать приложения по просьбе незнакомцев и сразу звонить вам в подобных случаях.

– Михаил Михайлович, чего ни в коем случае нельзя делать при подозрительном звонке или СМС-сообщении?

– Чтобы не попасться на удочку злоумышленников, нельзя:

● сообщать персональные данные (Ф.И.О., паспортные данные, СНИЛС, адрес и т.д.);

● называть одноразовые коды из телефонных сообщений;

● сканировать чужие QR-коды;

● устанавливать неизвестные приложения и программы;

● перезванивать по номерам, указанным в подозрительном сообщении;

● предоставлять доступ к экрану мобильного телефона;

● переводить деньги по требованию звонящего;

● сообщать номера банковских карт, кодовое слово и пин-код.

– Я бы ещё добавила: не участвуйте в голосованиях по присланной ссылке.

– Полностью поддерживаю. При переходе по непроверенным ссылкам может автоматически скачаться вирус или открыться фишинговый сайт – это сайт-двойник очень похожий на настоящий сайт банка, поликлиники и т.д. Если ввести там логин, пароль или

данные карты, их украдут мошенники.

Если гражданин назовёт цифровой код или пин-код, то злоумышленники смогут получить доступ к его мобильному банку либо банковской карте. Код может подтвердить оформление кредита или списание средств со счёта. Или он нужен преступникам, чтобы получить доступ к личному кабинету на портале «Госуслуг».

Если во время звонка что-то показалось вам подозрительным, просто положите трубку и не отвечайте на вопросы неизвестных. Не вступайте с ними в дискуссию – преступники могут записать ваш голос и сделать на его основе «речевого двойника». Потом этот поддельный голос могут использовать для отправки голосовых сообщений, например, «Надо срочно проголосовать за мою дочь, не хватает пары голосов». Люди, которые слышат такое сообщение от «знакомого», часто не подозревают подмены и переходят по ссылке.

По этой же причине старайтесь не произносить по телефону каких-либо подтверждающих слов («да», «согласен», «подтверждаю»), чтобы мошенники не могли использовать эти фразы в своих целях.

Если вам предлагают «быстро», «срочно», «немедленно» что-то сделать – сделайте паузу. При подозрении на мошенничество сохраните скриншоты сообщений и записи звонков, заблокируйте номер и обратитесь в банк (если речь идет о платежах) и в полицию. Не поддавайтесь давлению, при любых сомнениях проверяйте полученную информацию через официальные источники. Эти простые, но эффективные меры уберегут вас и ваших близких от большинства мошеннических схем.

НЕ ЗНАЕТЕ, ГДЕ
ПОЛУЧИТЬ ОТВЕТ?

СПРОСИТЕ У «ТОМИ»!

Дорогие читатели!

Если у вас есть проблемы, пишите письма, звоните в редакцию – задавайте наиболее волнующие вопросы в «Справочную». Приглашаем вас принять участие в создании настоящей народной газеты, чтобы «ТОМЬ» стала лучше и интереснее.

- ✓ Обратитесь к нам с волнующей вас темой, а наши журналисты найдут ответ у компетентного специалиста.
- ✓ Присылайте нам письма на kemerovored@province.ru. Рассказывайте об интересных событиях, участниках и очевидцами которых вы стали, поделитесь злободневными темами, которые обсуждают сослуживцы и соседи.

Пишите: **650099, г. Кемерово, пр. Ленина 33/2, офис 310 Б.**
Звоните по телефону: **8 (3842) 45-21-17** (по будним дням с 10.00 до 17.00). e-mail: kemerovoredtom@mail.ru.

▲ Полосу подготовила Анна ШИНКАРЧУК